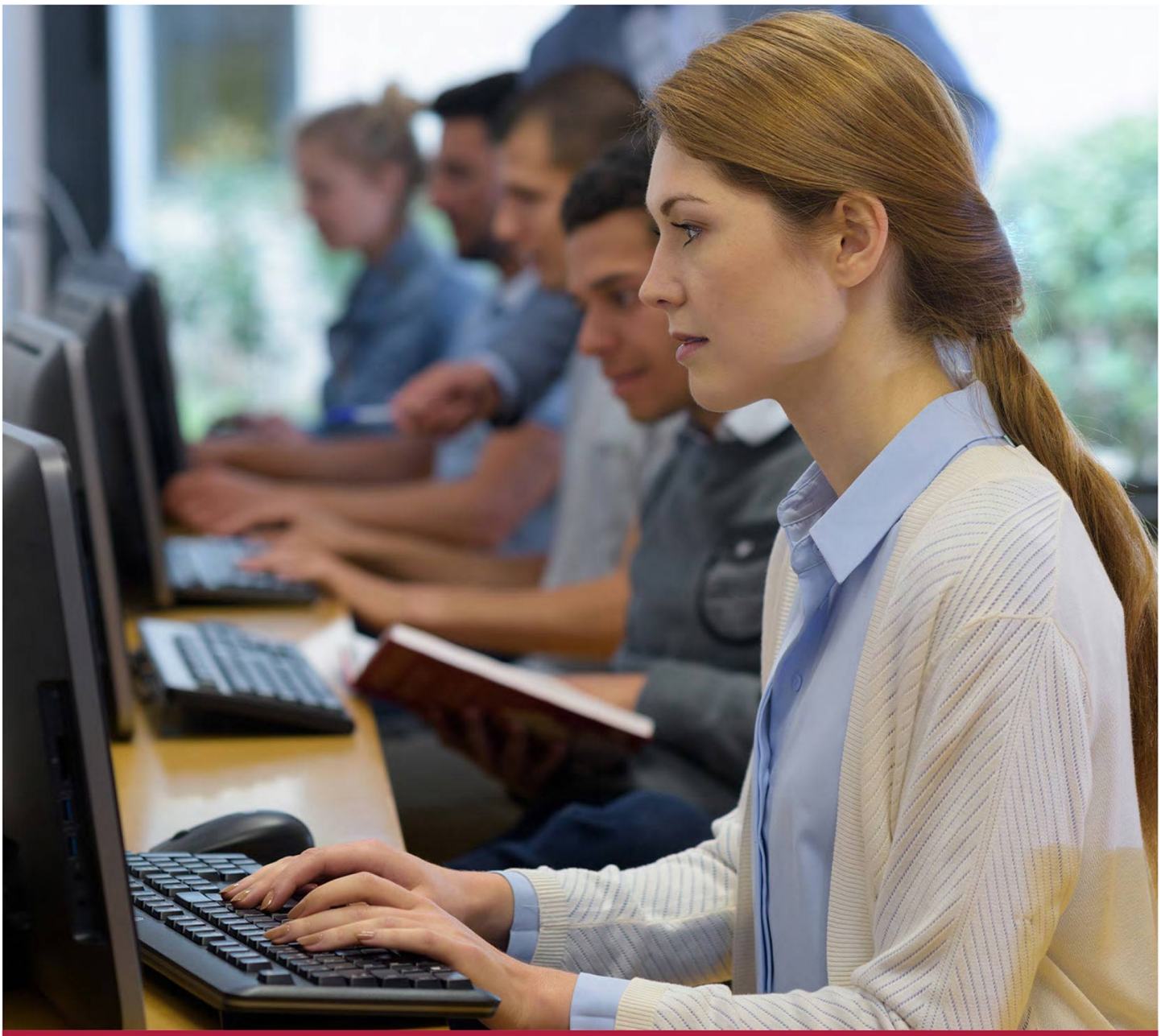
Академия АйТи
a Softline Company



Безопасность облачных технологий

Код курса: cloud_sec

+7 (495) 150 96 00 | academy@academyit.ru | academyit.ru

Безопасность облачных технологий

Код курса: cloud_sec

Длительность	40 ак. часов
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Массовый переход бизнеса на облачные инфраструктуры многократно расширил поверхность для кибератак, сделав защиту распределенных данных абсолютным приоритетом. Специфика облачных сред требует кардинально иного подхода к управлению рисками, где малейшая ошибка в конфигурациях может привести к катастрофическим утечкам. Формирование глубокой внутренней экспертизы в области облачной безопасности перестало быть сугубо технической задачей, трансформировавшись в фундаментальное условие для устойчивого развития современного бизнеса. Облачная безопасность требует отдельного фокуса, поскольку защита теперь строится не на классических межсетевых экранах, а на тонкой настройке систем идентификации (IAM), прав доступа к API и изоляции контейнеров. Именно поэтому бизнесу нужны инженеры, способные не просто администрировать системы, а «зашивать» политики безопасности прямо в код инфраструктуры (IaC) и выстраивать модель «нулевого доверия» (Zero Trust) для каждого микросервиса.

Подробная информация

Профиль аудитории:
• Специалисты информационной безопасности
• Системные и сетевые администраторы и инженеры, касающиеся вопросов обеспечения информационной безопасности инфраструктуры
• DevOps-инженеры
• Архитекторы облачных решений
Предварительные требования:
• Базовые знания сетевых технологий (TCP/IP)
• Понимание принципов работы Linux/Windows систем
• Понимание базовых концепций обеспечений информационной безопасности
По окончании курса слушатели изучат:
• Определять границы зон ответственности между клиентом и облачным провайдером;
• Проектировать безопасную архитектуру сетей (VPC) и настраивать межсетевые экраны в облаке;
• Управлять доступом пользователей (IAM) и настраивать многофакторную аутентификацию;
• Обеспечивать безопасность облачных объектных хранилищ и бакетов;
• Защищать веб-приложения с помощью WAF и интегрировать безопасность в CI/CD (DevSecOps);

• Проводить аудит безопасности, собирать логи и реагировать на облачные инциденты;
• Применять требования российского законодательства (152-ФЗ, КИИ) к облачной ИТ-инфраструктуре.

Программа курса

Тема 1. Архитектура облаков и модели угроз

- Модели развертывания (IaaS, PaaS, SaaS) и их специфика
- Разделение ответственности (Shared Responsibility Model) провайдера и клиента
- Ландшафт актуальных облачных угроз и рисков
- Практическая работа: Развертывание базовой инфраструктуры и построение модели угроз

Тема 2. Сетевая безопасность в облачной среде

- Проектирование виртуальных сетей (VPC) и изоляция подсетей
- Настройка облачных межсетевых экранов (NGFW) и Security Groups
- Методы противодействия DDoS-атакам и защита периметра
- Организация защищенного удаленного доступа (VPN, концепция Zero Trust)
- Практическая работа: Сегментация сети, фильтрация трафика и симуляция отражения DDoS

Тема 3. Управление доступом (IAM) и защита данных

- Сервисы идентификации и контроля доступа (IAM), роли и политики
- Настройка многофакторной аутентификации (MFA) и Identity Hub
- Безопасность облачных хранилищ и настройка доступов к бакетам
- Шифрование данных (At-Rest / In-Transit) и управление ключами (KMS)
- Практическая работа: Настройка ролевой модели (RBAC) и защита объектного хранилища

Тема 4. Безопасность приложений и DevSecOps в облаке

- Специфика уязвимостей облачных сервисов (OWASP Top 10)
- Межсетевые экраны уровня приложений (WAF)
- Концепция Shift-Left и внедрение DevSecOps в CI/CD процессы
- Инструменты статического (SAST) и динамического (DAST) анализа кода
- Практическая работа: Развертывание WAF и интеграция сканера безопасности в пайплайн

Тема 5. Мониторинг, аудит и реагирование на инциденты

- Облачный мониторинг, сбор и логирование событий (Observability)
- Настройка сервисов аудита облачной инфраструктуры
- Жизненный цикл инцидента безопасности в облаке
- Основы облачной криминалистики (форензики) и поиск скрытых угроз
- Практическая работа: Настройка сбора логов, выявление аномалий и разбор кейса взлома учетной записи

Тема 6. Комплаенс, стандарты и итоговая аттестация

- Регуляторные требования РФ (152-ФЗ, КИИ, ГОСТ алгоритмы)

- Международные стандарты безопасности облаков (ISO 27017, CSA)
- Составление ТЗ на услуги безопасного облачного провайдера
- Практическая работа: Итоговое тестирование и защита комплексного проекта по защите облака

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

+7 (495) 150 96 00 | academy@academyit.ru